Could, or *should* the ancient Greeks have discovered the Lucas-Lehmer test?

ROBERT GRANGER

1 Introduction

The Lucas-Lehmer (LL) test is the most efficient known for deterministically testing the primality of Mersenne numbers, i.e., the integers $M_l = 2^l - 1$, for $l \geq 1$. The Mersenne numbers are so-called in honour of the French scholar Marin Mersenne (1588-1648), who in 1644 published a list of exponents $l \leq 257$ which he conjectured produced all and only those M_l which are prime, for l in this range, namely[1] $l = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ and 257 [1]. Mersenne's list turned out to be incorrect, omitting the prime-producing $l = 61, 89$ and 107 and including the composite-producing $l = 67$ and 257, although this was not finally confirmed until 1947, using both the LL test and contemporary mechanical calculators [2]. The LL test is based on the following theorem.

Theorem 1.1. *[3, 4] Define a sequence of integers x_k by the recursion*

$$x_0 = 4, \quad x_{k+1} = x_k^2 - 2. \tag{1}$$

Then $M_l = 2^l - 1$ is prime if and only if $M_l \mid x_{l-2}$.

When first encountered, this test may seem astonishing, giving the uninitiated virtually no hint as to why it is correct. Indeed, despite being developed by Lucas — albeit in a slightly different form — in 1876 [3], it was not until Lehmer's above formulation and proof in 1930 [4] that the condition of the test was rigorously shown to be both necessary and sufficient. In particular, the idea behind the test almost seems to have been deliberately obfuscated, though admittedly this in no small way contributes to its elegance. However, once a key idea is understood, it is fairly straightforward to prove Theorem 1.1 with only a modicum of abstract algebra.

In this article, we argue that the LL test could in principle have been discovered by the ancient Greeks, rather than arising as it did as a consequence of Lucas' brilliant insights. Our argument is based on two derivations together with supporting observations. Firstly, we demonstrate how the LL test may be naturally extrapolated from Heron's 1$^{\text{st}}$ century method for computing square roots when used to compute $\sqrt{3}$. Indeed, so naturally does the test arise from this computation, that we contend that a 1$^{\text{st}}$ century mathematician could feasibly have discovered it. Moreover, in the 3$^{\text{rd}}$ century BC, Archimedes had already computed rational approximations to $\sqrt{3}$ for his estimate of π [5,

[1] Note that for M_l to be prime, l itself must be prime, since if $a \mid l$, then $(2^a - 1) \mid (2^l - 1)$.

p. 51], and so mathematicians of the era were certainly well motivated to consider this problem. Secondly, although a matter of some historical debate, the upper and lower bounds produced by Archimedes may also imply a knowledge of the continued fraction method of approximating square roots — since they are convergents — a method which was not published until 1572 by Bombelli [6], and which as we show also leads to the LL test. Finally, interest in Mersenne primes would have no doubt been piqued by Euclid's well-known theorem on even perfect numbers [7, Book IX, Prop. 36], and so one expects that contemporary mathematicians would have been 'primed' to make the discovery, had they carried out either of the above computations. Taking each of these factors into account, one is naturally led to ask not so much whether the LL test *could* have been discovered by the ancient Greeks, but whether the LL test *should* have been discovered? It is of course anachronistic to impose upon hypothetical ancient scholars a facility with the techniques of modern mathematics; however, we readily invite the reader to make their own assessment as to the merits of our argument.

While we do not believe a proof would have been within the reach of the mathematics of the time, it is nevertheless tantalising to consider the possibility that *had* the LL test been discovered, then the notions required to prove it might also have been found, if not by the ancient Greeks, then at least at some time prior to its formulation more than two millennia later.

In addition to our central argument, we present a new, simple and arguably more natural variant of the LL test, which arises directly from both Heron's method and continued fractions. We also explicate the key idea behind Theorem 1.1, and briefly explore how various representations of the underlying group involved give rise to equivalent formulations.

2 Discovering the Lucas-Lehmer test via Heron's method

One way to compute the square root of an integer, or rather rational approximations thereto, is to use Heron's method [5, pp. 323–324], named after the 1st century Greek mathematician Heron of Alexandria. This method was very probably also known to the Babylonians [8].

To compute successive approximations to $\sqrt{D}$, one starts with any initial positive value x'_0 (usually $\lfloor\sqrt{D}\rfloor$, the largest integer $\leq \sqrt{D}$), and defines a sequence of rationals x'_k by:

$$x'_{k+1} = \frac{1}{2}\Big(x'_k + \frac{D}{x'_k}\Big). \tag{2}$$

It is easy to show that $\lim_{k\to\infty} x'_k = \sqrt{D}$, and that the convergence is quadratic. Note that Heron's method is identical to Newton's iteration for solving the equation $f(x) = x^2 - D = 0$.

We start by considering the sequence x'_k of rationals given by Heron's method for computing $\sqrt{3}$, which for $x'_0 = \lfloor\sqrt{3}\rfloor = 1$, begins

$$[1,\ 2,\ 7/4,\ 97/56,\ 18817/10864,\ 708158977/408855776,\ 1002978273411373057/579069776145402304, \ldots]. \tag{3}$$

Since each x'_k is rational, for $k \geq 1$ we write $x'_k = n_k/d_k$, with $n_1 = 2,\ d_1 = 1$. Writing recursion (2) in terms of (n_k, d_k) one has

$$x'_{k+1} = \frac{1}{2}\Big(x'_k + \frac{3}{x'_k}\Big) = \frac{1}{2}\Big(n_k/d_k + \frac{3}{n_k/d_k}\Big) = \frac{n_k^2 + 3d_k^2}{2n_k d_k},$$

and hence for $k \geq 1$ one can express recursion (2) equivalently as

$$n_1 = 2,\ d_1 = 1,\ n_{k+1} = n_k^2 + 3d_k^2,\ d_{k+1} = 2n_k d_k. \tag{4}$$

Testing the first few terms, it seems that $\gcd(n_k, d_k) = 1$ may be true for all $k \geq 1$, and indeed this is easily proven by induction (or as we show shortly). For this reason, or perhaps due to mathematical curiosity, it is natural to factor the first few terms. Noting that $d_k = 2^{k-1} \cdot \prod_{i=1}^{k-1} n_i$, we need only factor the n_k's. Starting from n_1, this gives the sequence:

$$[2,\ 7,\ 97,\ 31 \cdot 607,\ 708158977,\ 127 \cdot 7897466719774591, \ldots].$$

This is not much data to go on, however the keen observer will notice that $7 \mid n_2$, $31 \mid n_4$ and $127 \mid n_6$, or rather $(2^3 - 1) \mid n_2$, $(2^5 - 1) \mid n_4$ and $(2^7 - 1) \mid n_6$, but that $(2^4 - 1) \nmid n_3$ and $(2^6 - 1) \nmid n_5$.

Based on these five cases one might postulate that for $l \geq 3$, if $2^l - 1$ is prime then $(2^l - 1) \mid n_{l-1}$; and conversely, if $2^l - 1$ is composite then $(2^l - 1) \nmid n_{l-1}$. Perhaps annoyingly, this does not work for $l = 2$ (but for good reason, see §3.2), however this is no reason not to test further small cases — up to $l = 13$ for instance — for which the postulate is borne out. We thus have a very natural, but perhaps loosely supported conjecture, which we formalise as follows:

Conjecture 2.1. For $l \geq 3$ let $p = 2^l - 1$, and let the sequence n_k be given by recurrence (4). Then p is prime if and only if $p \mid n_{l-1}$.

So is Conjecture 2.1 the LL test? Well, in this form not quite, but one can relate the two with the following simple observation. Since n_k/d_k converges to $\sqrt{3}$, its square converges to 3. The 'error' in this approximation shrinks to zero as $k \to \infty$. In particular we have $n_1^2/d_1^2 = 3 + 1$, $n_2^2/d_2^2 = 3 + 1/4^2$, $n_3^2/d_3^2 = 3 + 1/56^2$, and it seems that for $k \geq 1$, one has

$$n_k^2/d_k^2 = 3 + 1/d_k^2,\ \text{or}\ n_k^2 - 3d_k^2 = 1.$$

This can be proven by induction by simply plugging in the formulae from recursion (4):

$$n_{k+1}^2 - 3d_{k+1}^2 = (n_k^2 + 3d_k^2)^2 - 3 \cdot (2n_k d_k)^2 = (n_k^2 - 3d_k^2)^2 = 1.$$

Hence the sequence of pairs (n_k, d_k) for $k \geq 1$ are actually integral solutions to the equation $x^2 - 3y^2 = 1$ (and so $\gcd(n_k, d_k) = 1$, as claimed). Neglecting for the moment that this is a Pell conic (the discussion of which we defer until §3.3), one deduces from this that the recursion for n_k may be rewritten as:

$$n_1 = 2,\ n_{k+1} = n_k^2 + 3d_k^2 = 2n_k^2 - 1. \tag{5}$$

Comparing (5) with (1), observe that $n_1 = x_0/2$, and by induction we have $n_{k+1} = 2n_k^2 - 1 = 2(x_{k-1}/2)^2 - 1 = (x_{k-1}^2 - 2)/2 = x_k/2$, and so accounting for the shift by one position, recursion (5) is simply half the LL recursion (1)! Furthermore, since $\gcd(p, 2) = 1$ we see that Conjecture 2.1 is equivalent to Theorem 1.1. Hence merely by computing $\sqrt{3}$ using Heron's method and making some very elementary observations, it is in principle possible to arrive at the LL test purely empirically.

2.1 Could the ancient Greeks have made this discovery?

We have shown that one could feasibly have stumbled upon Conjecture 2.1 without ever having been looking for a Mersenne number primality test. We now argue that a 1st century mathematician could plausibly have done so.

Firstly, computing square roots is a naturally interesting and relevant endeavour. Furthermore, as is well known, in the 3rd century BC Archimedes used the rational approximations [5, p. 51]

$$\frac{265}{153} < \sqrt{3} < \frac{1351}{780} \tag{6}$$

in his estimate of π. Hence there can be no doubt that this problem *was* addressed.

Secondly, once Heron's method was available, it would be the natural algorithm to use. Finally, assuming our hypothetical scholar was able to factor 18817, he could arguably have extrapolated Conjecture 2.1 from the three observations $(2^3 - 1) \mid n_2$, $(2^4 - 1) \nmid n_3$ and $(2^5 - 1) \mid n_4$ alone. He could then have tested the divisibility of n_{l-1} by $2^l - 1$ for larger l far more easily than he could have factored n_{l-1}. Furthermore, he may also have astutely observed that for a given l, the sequence $n_1, \ldots, n_{l-1}$ need only be computed mod $2^l - 1$, since only the remainder when n_{l-1} is divided by $2^l - 1$ is needed, thus making the computation far simpler. This is of course how one applies and implements Theorem 1.1 in practice. Using such observations he could then have checked the conjecture for other small l and used trial division to test the primality of $2^l - 1$, perhaps up to $2^{13} - 1 = 8191$ or even larger, and established sufficient grounds to confidently postulate Conjecture 2.1.

In actuality the Greeks were apparently only aware of primes of the form $2^l - 1$, for $l \leq 7$, which is somewhat surprising given that one would have expected their interest to have been piqued by Euclid's well-known theorem on even perfect numbers [7, Book IX, Prop. 36], which states that if $2^l - 1$ is prime, then $N = 2^{l-1}(2^l - 1)$ is perfect, i.e., the sum of its proper divisors equals N. While we do not attempt to explain the reasons for this, we believe it plausible that a mathematician who was aware of Euclid's theorem would have been 'primed' to discover the LL test, should he have carried out the above computation, or the one detailed next in §2.2.

We lastly remark that when Heron's method is used to compute rational approximations to $\sqrt{6}$, with $x_0' = \lfloor \sqrt{6} \rfloor = 2$, one obtains the following sequence of numerators n_k, for $k \geq 0$:

$$\begin{aligned}[2,\ 5,\ 7^2,\ 4801,\ 31 \cdot 1487071,\ 52609 \cdot 80789839489,\\ 127 \cdot 769 \cdot 36810112513 \cdot 10050007226929279, \ldots].\end{aligned} \tag{7}$$

As we found for $\sqrt{3}$, here one also has $(2^3 - 1) \mid n_2$, $(2^5 - 1) \mid n_4$ and $(2^7 - 1) \mid n_6$, and $(2^4 - 1) \nmid n_3$ and $(2^6 - 1) \nmid n_5$. While this does not readily apply to the square root of

all non-square integers, this is surely no coincidence! We believe this lends weight to our contention that a 1st century mathematician could feasibly have discovered the LL test.

2.2 Discovering the Lucas-Lehmer test via continued fractions

In this section we demonstrate how Heron's method when used to compute $\sqrt{3}$ is naturally related to the continued fraction expansion of $\sqrt{3}$, thus offering another possible avenue of discovery of the LL test.

The Greeks are known to have routinely used continued fractions — based on the ubiquitous Euclidean algorithm — in order to express rational numbers. When the Pythagoreans found these numbers to be inadequate to represent all quantities ($\sqrt{2}$ being the example *par excellence*), they were left with a *real* problem. However, in the 4th century BC, Eudoxos found a way to represent not only those quantities arising from Euclidean geometry, but *all* real numbers — as we call them today — by allowing arbitrary infinite continued fractions [9, p. 57].

The continued fraction for $\sqrt{3}$ may be represented as $[1;\overline{1,2}]$, where the bar means that the sequence $[1,2]$ is repeated indefinitely, and both the notation and the equality may be deduced from the equation

$$\sqrt{3}-1=\frac{1}{1+\frac{1}{2+(\sqrt{3}-1)}}. \tag{8}$$

It is very likely that the ancient Greeks knew how to expand the square root of positive integers as continued fractions, Theaetetos having established much of how to do this, as recorded in Book X of Euclid's Elements [7].

The sequence of convergents for $\sqrt{3}$ arising from (8) is

$$[1,2,\frac{5}{3},\frac{7}{4},\frac{19}{11},\frac{26}{15},\frac{71}{41},\frac{97}{56},\frac{265}{153},\frac{362}{209},\frac{989}{571},\frac{1351}{780},\ldots], \tag{9}$$

where the m-th term c_m equals the expansion of the m-term truncation of $[1;\overline{1,2}]$. Observe that $c_1=x'_0$, $c_2=x'_1$, $c_4=x'_2$, $c_8=x'_3$ and it appears that in general one has

$$c_{2^i}=x'_i. \tag{10}$$

Note Archimedes' lower and upper bounds for $\sqrt{3}$ from (6) also appearing in (9). Hence if continued fractions were indeed Archimedes' method of arriving at (6), then with a little more effort than is required when using Heron's method, the LL test could feasibly have been discovered by this approach as well, having the form '$p=2^l-1$ is prime if and only if p divides the numerator of $c_{2^{l-1}}$'.

One way to prove (10) is as follows. By the definition of convergents and using (8), we have $c_1=1, c_2=2$, and for $m\geq 1$:

$$c_{2m+2}-1=\frac{1}{1+\frac{1}{2+(c_{2m}-1)}},\qquad c_{2m+1}-1=\frac{1}{1+\frac{1}{2+(c_{2m-1}-1)}},$$

and hence

$$c_{2m+2}=\frac{2c_{2m}+3}{c_{2m}+2},\qquad c_{2m+1}=\frac{2c_{2m-1}+3}{c_{2m-1}+2}.$$

Letting $c_m = a_m/b_m$, with $a_1 = b_1 = b_2 = 1$ and $a_2 = 2$, upon expanding, for $m \geq 1$ this becomes

$$\left[\begin{array}{c} a_{2m+2} \\ b_{2m+2} \end{array} \right] = \left[\begin{array}{cc} 2 & 3 \\ 1 & 2 \end{array} \right] \left[\begin{array}{c} a_{2m} \\ b_{2m} \end{array} \right], \quad \left[\begin{array}{c} a_{2m+1} \\ b_{2m+1} \end{array} \right] = \left[\begin{array}{cc} 2 & 3 \\ 1 & 2 \end{array} \right] \left[\begin{array}{c} a_{2m-1} \\ b_{2m-1} \end{array} \right], \tag{11}$$

and hence

$$\left[\begin{array}{c} a_{2m+2} \\ b_{2m+2} \end{array} \right] = \left[\begin{array}{cc} 2 & 3 \\ 1 & 2 \end{array} \right]^m \left[\begin{array}{c} 2 \\ 1 \end{array} \right], \quad \left[\begin{array}{c} a_{2m+1} \\ b_{2m+1} \end{array} \right] = \left[\begin{array}{cc} 2 & 3 \\ 1 & 2 \end{array} \right]^m \left[\begin{array}{c} 1 \\ 1 \end{array} \right],$$

which also both hold for $m = 0$. For the LL test, one need only consider the even-terms recurrence. The eigenvalues of the 2×2 matrix appearing in (11) are $2 \pm \sqrt{3}$, which one can check leads to the solution, for $m \geq 1$:

$$\begin{aligned} a_{2m} &= ((2+\sqrt{3})^m + (2-\sqrt{3})^m)/2, \\ b_{2m} &= ((2+\sqrt{3})^m - (2-\sqrt{3})^m)/2\sqrt{3}, \end{aligned}$$

or

$$c_{2m} = \sqrt{3} \cdot \frac{(2+\sqrt{3})^m + (2-\sqrt{3})^m}{(2+\sqrt{3})^m - (2-\sqrt{3})^m}.$$

On the other hand, the odd-terms recurrence has solution, for $m \geq 0$:

$$\begin{aligned} a_{2m+1} &= ((1+\sqrt{3})(2+\sqrt{3})^m + (1-\sqrt{3})(2-\sqrt{3})^m)/2, \\ b_{2m+1} &= ((1+\sqrt{3})(2+\sqrt{3})^m - (1-\sqrt{3})(2-\sqrt{3})^m)/2\sqrt{3}, \end{aligned}$$

giving

$$c_{2m+1} = \sqrt{3} \cdot \frac{(1+\sqrt{3})(2+\sqrt{3})^m + (1-\sqrt{3})(2-\sqrt{3})^m}{(1+\sqrt{3})(2+\sqrt{3})^m - (1-\sqrt{3})(2-\sqrt{3})^m}.$$

In fact both expressions can be neatly tidied into a single one. Noting that

$$\left(\frac{1+\sqrt{3}}{1-\sqrt{3}} \right)^2 = \frac{2+\sqrt{3}}{2-\sqrt{3}},$$

for $m \geq 1$ we have

$$c_m = \sqrt{3} \cdot \frac{\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^m + 1}{\left(\frac{1+\sqrt{3}}{1-\sqrt{3}}\right)^m - 1}. \tag{12}$$

Equation (12) may also be rewritten in the convenient and attractive form

$$\frac{c_m + \sqrt{3}}{c_m - \sqrt{3}} = \left(\frac{1+\sqrt{3}}{1-\sqrt{3}} \right)^m. \tag{13}$$

Given any two elements c_m, c_n of the sequence of convergents for $\sqrt{3}$, equation (13) enables one to compute c_{m+n} easily:

$$c_{m+n} = \left(\frac{1+\sqrt{3}}{1-\sqrt{3}} \right)^{m+n} = \left(\frac{c_m + \sqrt{3}}{c_m - \sqrt{3}} \right) \cdot \left(\frac{c_n + \sqrt{3}}{c_n - \sqrt{3}} \right) = \left(\frac{\frac{c_m c_n + 3}{c_m + c_n} + \sqrt{3}}{\frac{c_m c_n + 3}{c_m + c_n} - \sqrt{3}} \right), \tag{14}$$

and hence

$$c_{m+n} = \frac{c_m c_n + 3}{c_m + c_n}. \tag{15}$$

The set of convergents $C = \{c_m\}_{m\geq 1}$ forms what is technically known as an infinite cyclic semigroup $(C, \oplus)$ with generator c_1, where the group operation $\oplus$ is defined by $c_m \oplus c_n = c_{m+n}$, which is given by (15). The semigroup $(C, \oplus)$ is therefore isomorphic to $(\mathbb{Z}_{\geq 1}, +)$, the set of positive integers under addition. Furthermore, by allowing $m \leq 0$ on the right-hand-side of (13), one can extend the set of convergents to form an isomorphism with all of $(\mathbb{Z}, +)$; this results in $c_m = -c_{-m}$ for $m < 0$, and $c_0 = \infty$, which should be interpreted in the following manner:

$$\frac{\infty + \sqrt{3}}{\infty - \sqrt{3}} = 1.$$

However, we shall only be interested in $m \geq 0$. What the above considerations show is that recursion (2) in Heron's method is just the doubling formula in $(C, \oplus)$, since (15) gives

$$c_m \oplus c_m = c_{2m} = \frac{c_m^2 + 3}{2c_m} = \frac{1}{2}\Big(c_m + \frac{3}{c_m}\Big),$$

which finally proves (10).

Incidentally, Lehmer's proof of the LL test makes essential use of two sequences of integers very similar to our a_m, b_m. In particular, for $m \geq 1$ let

$$V_m = (1+\sqrt{3})^m + (1-\sqrt{3})^m \quad \text{and} \quad U_m = ((1+\sqrt{3})^m - (1-\sqrt{3})^m)/2\sqrt{3}.$$

One can easily check that for $m \geq 1$, we have $a_m/b_m = c_m = V_m/2U_m$. Regarding the various proofs of the LL test, Tao has observed that 'they are sometimes presented in a way that involves pulling a lot of rabbits out of hats, giving the argument a magical feel rather than a natural one' [10]. One may agree that in accordance with this view, Lehmer's proof [4] does indeed seem quite unmotivated; see also [11, 12]. However, when seen in the context of our new, simple and well-motivated formulation of the LL test, the above connection between V_m, U_m and the continued fraction expansion of $\sqrt{3}$ provides one explanation as to how (and why) Lehmer's proof arises.

3 A more natural variant of the Lucas-Lehmer test?

In this section we present a variant of the LL test, along with a proof derived from insights developed in §2.2.

Theorem 3.1. *For $l \geq 3$ let $p = 2^l - 1$ and define a sequence of elements of $\mathbb{Z}/p\mathbb{Z}$ by the recursion*

$$\bar{x}_0 \equiv 1, \quad \bar{x}_{k+1} \equiv \frac{1}{2}\Big(\bar{x}_k + \frac{3}{\bar{x}_k}\Big) \pmod{p}. \tag{16}$$

Then p is prime if and only if $\bar{x}_{l-1}$ exists and $\bar{x}_{l-1} \equiv 0 \pmod{p}$.

Note that by $1/\bar{x}$ we mean the modular inverse of $\bar{x}$ in $\mathbb{Z}/p\mathbb{Z}$ (if it exists), i.e., the unique element $\bar{y} \in \mathbb{Z}/p\mathbb{Z}$ for which $\bar{x} \cdot \bar{y} \equiv 1 \pmod{p}$. For example, $1/2 \equiv 2^{l-1} \pmod{p}$ since $2 \cdot 2^{l-1} = 2^l \equiv 1 \pmod{p}$. In general the modular inverse of $\bar{x}$ exists if and only if $\gcd(\bar{x}_k, p) = 1$, and can be found using the Extended Euclidean Algorithm [13, Alg. X, p. 325], or [14, §2.4], for example. Provided that inverses exist, all the usual rules of arithmetic in $\mathbb{Q}$ such as cancellation and cross-multiplication apply in $\mathbb{Z}/p\mathbb{Z}$; when p is prime, every non-zero element has an inverse and $\mathbb{Z}/p\mathbb{Z}$ is the finite field $\mathbb{F}_p$, for which operations are exactly as they are in $\mathbb{Q}$. Computing $\bar{x}_{k+1}$ then just involves a multiplication of this inverse by 3, an addition and a modular division by 2, which can be effected in binary as a cyclic bitshift to the right by one place, as is easily verified. Hence, in order for $\bar{x}_{l-1}$ to be defined, we require that for $1 \leq k \leq l-2$, each $\bar{x}_k$ must be invertible mod p. If any $\bar{x}_k$ is not invertible mod p, then computing $\gcd(\bar{x}_k, p)$ will immediately give a factor of p, which gives even more information than simply proving that p is not prime. However, the chance of this occurring for a given l is extremely small.

The reader will of course have noticed that recursion (16) is simply Heron's method for computing $\sqrt{3}$ as given by (2) and in (3), taken mod p. So how might one go about proving Theorem 3.1? The only ingredients we need are some of the observations from §2.2 and a handful of results from elementary number theory and abstract algebra. For completeness, we now recall these results and some prerequisite definitions, which may be found in any introductory texts in the areas, see for example [15] and [16].

- (Quadratic residues): For q a prime and a not divisible by q, if the congruence

$$x^2 \equiv a \pmod{q}$$

  is soluble then a is called a *quadratic residue* mod q; otherwise a is a *quadratic nonresidue* mod q.

- (Legendre symbol): For q an odd prime, the values of the Legendre symbol $(\cdot/q)$ are given by

$$(a/q) = \begin{cases} +1 & \text{if } q \nmid a \text{ and } a \text{ is a quadratic residue mod } q \\ 0 & \text{if } q \mid a \\ -1 & \text{if } q \nmid a \text{ and } a \text{ is a quadratic nonresidue mod } q \end{cases}$$

- (Euler's criterion): For q an odd prime and any a we have

$$(a/q) \equiv a^{(q-1)/2} \pmod{q}.$$

- (Characterisation of $(3/q)$ and $(-2/q)$): For q an odd prime we have

$$(3/q) = \begin{cases} +1 & \text{if } q \equiv \pm 1 \pmod{12} \\ -1 & \text{if } q \equiv \pm 5 \pmod{12} \end{cases}, \quad (-2/q) = \begin{cases} +1 & \text{if } q \equiv 1, 3 \pmod{8} \\ -1 & \text{if } q \equiv 5, 7 \pmod{8} \end{cases}.$$

- (Finite fields): As stated above, if q is prime then $\mathbb{Z}/q\mathbb{Z}$ is the finite field $\mathbb{F}_q$. Furthermore if $(a/q) = -1$, then

$$\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{a}) = \{x + y\sqrt{a} \mid x, y \in \mathbb{F}_q\}$$

  is the finite field of q^2 elements. Observe that the multiplicative inverse of $x + y\sqrt{a}$ is $(x - y\sqrt{a})/(x^2 - ay^2)$, with the denominator non-zero since $(a/q) = -1$. We denote the multiplicative groups of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ by $\mathbb{F}_q^\times$ and $\mathbb{F}_{q^2}^\times$ respectively, which are both cyclic groups.

- (Lagrange's theorem): Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G. In particular, for any $g \in G$ the order of the subgroup generated by g divides the order of G.

3.1 A proof of Theorem 3.1

We begin with a few observations. Combining (10) and (13), for $k \geq 0$ we have (over $\mathbb{Q}$)

$$\frac{x'_k + \sqrt{3}}{x'_k - \sqrt{3}} = \left(\frac{1 + \sqrt{3}}{1 - \sqrt{3}}\right)^{2^k}. \tag{17}$$

Note that (17) is also derivable directly from recurrence (2) alone, independently of our consideration of continued fractions. For the sake of generality, consider (17) mod q for q any prime for which $(3/q) = -1$. We therefore have $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{3})$, and in this extension field, by Euler's criterion we have

$$\sqrt{3}^q = 3^{(q-1)/2} \cdot \sqrt{3} = -\sqrt{3}.$$

Hence for any $x \in \mathbb{F}_q$ we have

$$\left(\frac{x + \sqrt{3}}{x - \sqrt{3}}\right)^{q+1} = \frac{x - \sqrt{3}}{x + \sqrt{3}} \cdot \frac{x + \sqrt{3}}{x - \sqrt{3}} = 1.$$

Since elements of $\mathbb{F}_{q^2}$ of the form $(x + \sqrt{3})/(x - \sqrt{3})$ for $x \in \mathbb{F}_q$ are distinct (if $(x + \sqrt{3})/(x - \sqrt{3}) = (y + \sqrt{3})/(y - \sqrt{3})$ then $x = y$, as is easily verified by cross-multiplying), counting also the multiplicative identity element, we have a compact representation for the group of all $q + 1$ solutions in $\mathbb{F}_{q^2} = \mathbb{F}_q(\sqrt{3})$ to the equation $\alpha^{q+1} = 1$, which we denote by G_{q+1}. Note that arithmetic in G_{q+1} is exactly the same as it is for the set of convergents $C = \{c_m\}_{m \in \mathbb{Z}}$, with multiplication following from the third equality of (14), and inversion given by $((x + \sqrt{3})/(x - \sqrt{3}))^{-1} = (-x + \sqrt{3})/(-x - \sqrt{3})$. Furthermore, since G_{q+1} is a subgroup of the cyclic group $\mathbb{F}_{q^2}^\times$, it too is cyclic. Observe that the only element of order 2 in G_{q+1} has $x = 0 \in \mathbb{F}_q$, since

$$\left(\frac{x + \sqrt{3}}{x - \sqrt{3}}\right)^2 = 1 \iff x \equiv 0 \pmod{q}. \tag{18}$$

We have the following lemma.

Lemma 3.2. *For any prime $q \equiv 7 \pmod{24}$, the element $g = \frac{1+\sqrt{3}}{1-\sqrt{3}} \in G_{q+1}$ is not the square of another element in G_{q+1}.*

Proof. Suppose for $x \in \mathbb{F}_q$ that

$$\left(\frac{x+\sqrt{3}}{x-\sqrt{3}}\right)^2 = g.$$

Then x satisfies $x^2 - 2x + 3 = 0$, or $x = 1 \pm \sqrt{-2}$. However, $(-2/q) = -1$ for $q \equiv 7 \pmod 8$ and so no such $x \in \mathbb{F}_q$ exists. □

We are now ready to present our proof of Theorem 3.1.

Proof. Assume p is prime. Since $p \equiv 7 \pmod{24}$ we have $p \equiv 7 \pmod{12}$ and $p \equiv 7 \pmod 8$, and hence $(3/p) = -1$ and $(-2/p) = -1$ respectively. By Lemma 3.2, $g \in G_{p+1}$ is not a square and as $p + 1 = 2^l$ and G_{p+1} is cyclic, the order of g is 2^l. Hence $g^{2^{l-1}}$ has order 2 in G_{p+1} and so by (17) considered mod p, and (18), we have $\bar{x}_{l-1} \equiv 0 \pmod p$. Furthermore, no smaller power of g has order 2 and so by (18) again, $\bar{x}_k \not\equiv 0 \pmod p$ for $1 \le k \le l-2$ and hence $\bar{x}_{l-1}$ exists.

For the converse, suppose $\bar{x}_{l-1}$ exists and $\bar{x}_{l-1} \equiv 0 \pmod p$, and let q be a prime divisor of p, for which $(3/q) = -1$. Such a q always exists since otherwise, by the characterisation of $(3/q)$ one would have $p \equiv \pm 1 \pmod{12}$, whereas for odd l one has $p \equiv 7 \pmod{12}$. Then considering the entire sequence $\bar{x}_k \bmod q$, each element exists and $\bar{x}_{l-1} \equiv 0 \pmod q$. Hence by (18) we have $g^{2^{l-1}} = -1 \in G_{q+1}$, i.e., the order of g is $2^l = p+1$. By Lagrange's theorem we have $(p+1) \mid (q+1)$, and since $q \mid p$, we must have $q = p$, and so p is prime. □

3.2 Some remarks on the variant test

Firstly, observe that the above proof breaks when $l = 2$, since $3 \equiv 0 \pmod{2^2 - 1}$ and hence $g = 1$, which explains the exception noted in §2. Secondly, our variant test is slower than the original LL test, because of the modular inversions[2], so we do not propose that this method should be used in practice. Thirdly, while we have argued that the LL test could in principle have been discovered by the ancient Greeks (in the form of Conjecture 2.1), it should be evident that they almost certainly could not have proven its correctness, given the tools required to do so. Fourthly, as an exercise we invite the reader to prove the correctness of the corresponding variant test for $\sqrt{6}$ as given by (7) as well, using the above approach.

Furthermore, the key idea behind the test should now be clear from the proof of Theorem 3.1; it consists of simply checking the order of a particular element within a particular group. In particular, if p is prime then $g \in \mathbb{Z}/p\mathbb{Z}(\sqrt{3})$ has order $p+1$, from which one infers the necessity of the condition $\bar{x}_{l-1} \equiv 0 \pmod p$. Conversely, if g has order $p+1$ in $\mathbb{Z}/p\mathbb{Z}(\sqrt{3})$ then considering the sequence $\bar{x}_k \bmod q$ for a hypothetical divisor q of p with $(3/q) = -1$, the order of the subgroup G_{q+1} being $q+1$ forces $q = p$, from

[2] At asymptotic bitlengths the algorithm in [14, §2.4] for modular inversion in $\mathbb{Z}/(2^l-1)\mathbb{Z}$ is of the order of $\log l$ times slower than the fastest-known algorithm for squaring in $\mathbb{Z}/(2^l-1)\mathbb{Z}$ [17, Alg. 9.5.18].

which one infers the sufficiency of $\bar{x}_{l-1} \equiv 0 \pmod{p}$. This key idea is akin to the classical primality test due to Lucas, in which identifying an element of order $n-1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ proves that n is prime, since the order of $(\mathbb{Z}/n\mathbb{Z})^\times$ is $n-1$ if and only if n is prime. While this idea can be adapted for testing the primality of other integers, what makes it particularly simple for Mersenne numbers is that $p+1 = 2^l$, and so in order to identify a generator one only needs to find a non-square element in a suitable group, and likewise testing that the order of this element is $p+1$ only requires repeated squaring.

We can now tie everything together. Our proof of Theorem 3.1 shows that g has order $p+1 = 2^l$ in $\mathbb{Z}/p\mathbb{Z}(\sqrt{3})$ if and only if p is prime. Equivalently, we may state that g^{2^k} has order 2^{l-k} in $\mathbb{Z}/p\mathbb{Z}(\sqrt{3})$ if and only if p is prime. Observe that over $\mathbb{Q}$ we have $g^2 = 7 + 4\sqrt{3} = n_2 + d_2\sqrt{3}$ and $g^{2^k} = n_{k+1} + d_{k+1}\sqrt{3}$ for $k \geq 1$, with (n_k, d_k) defined exactly as in (4). Then letting $(\bar{n}_k, \bar{d}_k)$ be the mod p reduction of (n_k, d_k) and also using (5), we have $\bar{n}_{k+1} \equiv 2\bar{n}_k^2 - 1 \pmod{p}$ and $\bar{d}_{k+1} \equiv 2\bar{n}_k\bar{d}_k \pmod{p}$. Hence our proof can alternatively be expressed as $\bar{n}_{l-1} + \bar{d}_{l-1}\sqrt{3}$ has order 4 in $\mathbb{Z}/p\mathbb{Z}(\sqrt{3})$ if and only if p is prime. An element x of order 4 must satisfy $x^2 + 1 = 0 \in \mathbb{Z}/p\mathbb{Z}(\sqrt{3})$ and therefore

$$(\bar{n}_{l-1} + \bar{d}_{l-1}\sqrt{3})^2 + 1 = 2\bar{n}_{l-1}^2 - 1 + 2\bar{n}_{l-1}\bar{d}_{l-1}\sqrt{3} + 1 = \bar{n}_{l-1}(2\bar{n}_{l-1} + 2\bar{d}_{l-1}\sqrt{3}) = 0.$$

Thus $\bar{n}_{l-1} \equiv 0 \pmod{p}$ if and only if p is prime, proving Conjecture 2.1 and the original LL test, Theorem 1.1.

3.3 Connection with other proofs of the Lucas-Lehmer test

Our proof of Theorem 3.1 is very closely related to two other recent proofs of the LL test. While we do not go into all the details, for completeness we very briefly sketch these connections.

Firstly, the formulation of our proof of the LL test in terms of n_k, as just given above, is almost identical to that given by Gross in terms of the norm 1 algebraic torus associated to the real quadratic field $\mathbb{Q}(\sqrt{3})$ [18, Prop. 1.2-1.3]. The central difference between our proof and Gross' is the element representation we have chosen, which elucidates the connection with Heron's method and continued fractions.

Secondly, the definition of the algebraic torus just noted also happens to coincide with the definition of the Pell conic

$$\mathcal{P} = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} \mid x^2 - 3y^2 = 1\}.$$

As noted in §2, the sequence of pairs (n_k, d_k) for $k \geq 1$ are integral points on $\mathcal{P}$. The recursion for (n_k, d_k) is the point-doubling formula from a more general abelian group law which allows one to add any two points on $\mathcal{P}$. In particular, for $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ we have $P + Q = (x_P x_Q + 3y_P y_Q, x_P y_Q + x_Q y_P)$; observe that if we define $c_P = x_P/y_P$ and $c_Q = x_Q/y_Q$ then this group law is nothing but the one already derived for the convergents of $\sqrt{3}$ in (15). As was shown by Lemmermeyer, the LL test arises when checking the order of the point $P = (2, 1)$ on the mod p reduction of this group of points [19, Prop. 4]. Furthermore, by using a rational parameterisation of $\mathcal{P}$ which goes back perhaps as far as Diophantus [20, §1], one obtains an LL-style test based on Heron's method for computing $-1/\sqrt{3}$ with $x_0 = -2/3$, akin to Theorem 3.1.

4 Concluding remarks

In this expository article we have argued that the LL test could have been discovered naturally when computing rational approximations to $\sqrt{3}$, and that the ancient Greek mathematicians could feasibly have done so. We have also proven a natural and well-motivated variant of the LL test which arises from Heron's method and continued fractions, and briefly described its connection with other proofs of the original LL test.

In addition to the algebraic torus interpretation of the LL test, Gross has provided another test for the primality of Mersenne numbers based on the successive doubling of a point on the elliptic curve $y^2 = x^3 - 12x$ over $\mathbb{Q}$ [18, Prop. 2.2], which we state mod p.

Theorem 4.1. *For $l \geq 3$ let $p = 2^l - 1$ and define a sequence of elements of $\mathbb{Z}/p\mathbb{Z}$ by the recursion*

$$x_0 \equiv -2, \quad x_{k+1} \equiv \frac{(x_k^2 + 12)^2}{4x_k \cdot (x_k^2 - 12)} \pmod{p}.$$

Then p is prime if and only if x_{l-1} exists and $x_{l-1} \equiv 0 \pmod{p}$.

As with Theorem 3.1, the elliptic curve test is slower than the original LL test, and it seems unlikely that any primality test of Mersenne numbers based on checking the order of special elements will ever be faster.

Finally, we remark that at the time of writing there are 47 known Mersenne primes, the largest of which is $2^{43,112,609} - 1$; should the reader wish to assist in finding others we refer them to `www.mersenne.org`, which hosts the Great Internet Mersenne Prime Search. While it is conjectured that there are infinitely many Mersenne primes — Wagstaff has heuristically estimated that the number of Mersenne primes $\leq x$ tends to $(e^\gamma / \log 2) \log\log x$ as $x \to \infty$, where γ is the Euler-Mascheroni constant [21] — a proof of this natural conjecture still seems very far from reach.

Acknowledgements

The author would like to thank Rod Gow for his comments on an earlier draft of this article, and the reviewer for their many helpful suggestions.

References

[1] M. Mersenne. Cogitata Physico Mathematica, Parisiis, 1644. Praefatio Generalis No. 19.

[2] H.S. Uhler. ON ALL OF MERSENNE'S NUMBERS PARTICULARLY M_{193}. Nat. Acad. Sci., Proc., v. 34, Mar. 1948, pp. 102–103.

[3] E. Lucas. Nouveaux théorèmes darithmétique supérieure. C. R. Acad. Sci. Paris, 83, 1876, pp. 1286–1288.

[4] D.H. Lehmer. On Lucas's test for the primality of Mersenne's numbers. J. London Math. Soc., 10, 1935, pp. 162–165.

[5] T.L. Heath. A History of Greek Mathematics, Vol. 2. Oxford: Clarendon Press, 1921.

[6] R. Bombelli. L'Algebra. 1572.

[7] T.L. Heath. The thirteen books of Euclid's Elements, Cambridge University Press, 1908.

[8] D. Fowler and E. Robson. Square Root Approximations in Old Babylonian Mathematics: YBC 7289 in Context. Historia Mathematica 25, 1998, pp. 366–378.

[9] R. Penrose. The Road to Reality: A Complete Guide to the Laws of the Universe. Vintage, 2005.

[10] T. Tao. The Lucas-Lehmer test for Mersenne primes. Available from `http://terrytao.wordpress.com`

[11] M.I. Rosen. A proof of the Lucas-Lehmer test. The American Mathematical Monthly, Vol. 95, 1988, pp. 855–856.

[12] J.W. Bruce. A Really Trivial Proof of the Lucas-Lehmer Test. The American Mathematical Monthly, Vol. 100, 1993, pp. 370–371.

[13] D.E. Knuth. The Art of Computer Programming, v. 2. Seminumerical Algorithms. Addison-Wesley, 2nd edition, 1981.

[14] D. Stehlé and P. Zimmermann. A Binary Recursive Gcd Algorithm. Algorithmic Number Theory (ANTS-VI), LNCS 3076, Springer, 2004, pp. 411–425.

[15] G.H. Hardy and E.M. Wright. An introduction to the theory of numbers. The Clarendon Press, Oxford University Press, New York, 1979.

[16] I.N. Herstein. Abstract Algebra (3rd edition). John Wiley & Sons, 1996.

[17] R.E. Crandall and C. Pomerance. Prime Numbers: a computational perspective. Second edition, Springer, New York, 2005.

[18] B.H. Gross. An elliptic curve test for Mersenne primes. J. Number Theory, 110, 2005, pp. 114–119.

[19] F. Lemmermeyer. Conics - A Poor Man's Elliptic Curves. Preprint, 2003.

[20] F. Lemmermeyer. Circles, Primes and Quadratic Residues. Preprint, 1999.

[21] S.S. Wagstaff Jr. Divisors of Mersenne numbers. Math. Comp., 40, 1983, pp. 385–397.

ROBERT GRANGER
School of Mathematical Sciences
University College Dublin, Ireland
email: `robbiegranger@gmail.com`